Constructing permutations of finite fields via linear translators

Gohar M. Kyureghyan

Department of Mathematics, Otto-von-Guericke-University Magdeburg,
D-39016 Magdeburg, Germany

Abstract

We study the permutations of the finite field $\mathbb{F}_{q^n}$ given by $x + \gamma f(x)$, where $\gamma \in \mathbb{F}_{q^n}$ is a linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. We determine the cycle structure and the inverse of such a permutation. We describe several families of permutation polynomials obtained using functions with linear translators.

Keywords: Permutation polynomial, cycle structure, complete mapping, linear translator, linear structure.

1 Introduction

Let q be a power of a prime number and $\mathbb{F}_{q^n}$ be the finite field of order q^n. Any polynomial $F(X) \in \mathbb{F}_{q^n}[X]$ defines a mapping $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ via $x \mapsto F(x)$, which is called the associated mapping of $F(X)$. Furthermore, any mapping from a finite field into itself is given by a polynomial. A polynomial $F(X)$ is called a *permutation polynomial* of $\mathbb{F}_{q^n}$ if its associated mapping is a permutation. Permutation polynomials over finite fields have a variety of theoretical and practical applications. Permutations described by "nice", for instance sparse, polynomials are of special interest.

A permutation F, for which the mapping $G(x) = F(x) + x$ is a permutation as well, is called a *complete mapping*, while the mapping $G(x)$ in its turn is called an *orthomorphism*. Orthomorphisms yield latin squares which are orthogonal to the Caley table of the additive group of $\mathbb{F}_{q^n}$. More generally, let $H : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and define

$$\mathcal{M}(H) := \{c \in \mathbb{F}_{q^n} \mid H(x) + cx \text{ is a permutation of } \mathbb{F}_{q^n}\}.$$

Clearly, F is a complete mapping if and only if $\{0, 1\} \subseteq \mathcal{M}(F)$, and G is an orthomorphism if and only if $\{0, -1\} \subseteq \mathcal{M}(G)$. The set D_H of directions determined by the mapping H is defined as follows

$$D_H := \left\{ \frac{H(x) - H(y)}{x - y} \mid x, y \in \mathbb{F}_{q^n}, x \neq y \right\}.$$

Note that $c \in \mathcal{M}(H)$ if and only if $-c \notin D_H$, and hence a mapping H with a large set $\mathcal{M}(H)$ determines a small number of directions, or equivalently a small blocking set of Rédei type in $PG(2, q^n)$. Sharp bounds on the size of $\mathcal{M}(H)$ are proved in [1, 5, 10]. Further references on this topic may be found in [1].

Let $\gamma \in \mathbb{F}_{q^n}$ and $G : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n},\ f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and define

$$F(x) = G(x) + \gamma\, f(x). \tag{1}$$

The description of the mappings F and G with respect to a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ containing the element $\gamma \neq 0$ yields a geometrical relation between them. Indeed, let $(\gamma, \beta_1, \ldots, \beta_{n-1})$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Denote by $g_i : \mathbb{F}_{q^n} \to \mathbb{F}_q,\ 0 \leq i \leq n-1$, the coordinate functions of G with respect to the chosen basis. Then for any $x \in \mathbb{F}_{q^n}$ it holds

$$G(x) = g_0(x)\gamma + g_1(x)\beta_1 + \ldots + g_{n-1}(x)\beta_{n-1}$$

and

$$F(x) = (g_0 + f)(x)\gamma + g_1(x)\beta_1 + \ldots + g(x)\beta_{n-1}.$$

Hence F is obtained from G by changing its γ-coordinate function. In [4] APN mappings and in [3, 2, 8] permutations of form (1) are studied.

This paper continues the study of permutations of form (1). In Section 2 we briefly introduce a concept of a linear translator. Further we characterize permutations $x + \gamma\, f(x)$ of $\mathbb{F}_{q^n}$, where $\gamma \in \mathbb{F}_{q^n}$ is a linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. In particular, we determine explicitly the inverse and the cycle structure of such a permutation. In Section 3 we describe explicit constructions of permutation polynomials based on the results of Section 2. Moreover, we show that the knowledge of the inverse mapping of a permutation $x \mapsto x + \gamma\, f(x)$ allows to construct permutations by changing two coordinate functions of the identity mapping. Finally, in Section 4 we give further constructions of permutation polynomials of the shape $L(X) + \gamma\, f(X)$, where $L(X)$ is a linearized polynomial and $\gamma \in \mathbb{F}_{q^n}$ and the polynomial $f(X) \in \mathbb{F}_{q^n}[X]$ induces a mapping into $\mathbb{F}_q$. In the constructions of Section 4 the element γ is not necessarily a linear translator of f.

2 Remarks on permutations $x + \gamma\, f(x)$

Let f be a mapping from a finite field $\mathbb{F}_{q^n}$ into its subfield $\mathbb{F}_q$. Such a mapping can be represented by $Tr(G(x))$ for some (not unique) mapping $G : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, where Tr is the trace mapping from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$ given by

$$Tr(y) = y + y^q + y^{q^2} + \cdots + y^{q^{n-1}}.$$

Indeed, we need just to choose the value of $G(x)$ to satisfy $Tr(G(x)) = f(x)$.

A non-zero element $\alpha \in \mathbb{F}_{q^n}$ is called an a-linear translator (or linear structure, cf. [3, 2]) for the mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ if

$$f(x + u\alpha) - f(x) = ua, \tag{2}$$

for all $x \in \mathbb{F}_{q^n}, u \in \mathbb{F}_q$ and some fixed $a \in \mathbb{F}_q$. Note that if (2) is satisfied then a is uniquely determined, more exactly, it holds $a = f(\alpha) - f(0)$. The next two results are proved in [6], see also [2].

Proposition 1 *Let $\alpha, \beta \in \mathbb{F}_{q^n}^*,\ \alpha + \beta \neq 0$ and $a, b \in \mathbb{F}_q$. If α is an a-linear translator and β is a b-linear translator of a mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, then*

$$\alpha + \beta \text{ is an } (a+b) - \text{linear translator of } f$$

and for any $c \in \mathbb{F}_q^*$

$$c \cdot \alpha \text{ is a } (c \cdot a) - \text{linear translator of } f.$$

In particular, if $\Lambda^*(f)$ denotes the set of all linear translators of f, then $\Lambda(f) = \Lambda^*(f) \cup \{0\}$ is a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^n}$.

In particular Proposition 1 shows that the restriction of the mapping $f(x) - f(0)$ on the subspace $\Lambda(f)$ is a $\mathbb{F}_q$-linear mapping. So $\Lambda(f) = \mathbb{F}_{q^n}$ if and only if $f(x)$ is an affine mapping, or equivalently if $f(x) = Tr(\beta x) + b$ for some $\beta \in \mathbb{F}_{q^n}$ and $b \in \mathbb{F}_q$. Moreover, the following theorem holds:

Theorem 1 *Let $G : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and $f(x) = Tr(G(x))$. Then f has a linear translator if and only if there is a non-bijective $\mathbb{F}_q$-linear mapping $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ such that*

$$f(x) = Tr(G(x)) = Tr\big(H \circ L(x) + \beta x\big) \tag{3}$$

for some $H : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and $\beta \in \mathbb{F}_{q^n}$. In this case, the kernel of L is contained in the subspace $\Lambda(f)$.

By Theorem 1 any $\mathbb{F}_q$-linear mapping with a known kernel allows to construct a mapping with known linear translators. The following result is an example of this.

Lemma 1 *Let $H : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an arbitrary mapping, $\gamma, \beta \in \mathbb{F}_{q^n},\ \gamma \neq 0$. Then γ is a $Tr\big(\beta\gamma\big)$-linear translator of $f(x) = Tr(G(x))$ where*

$$G(x) = H(x^q - \gamma^{q-1}x) + \beta x.$$

Proof. Indeed, for any $u \in \mathbb{F}_q$ it holds

$$\begin{aligned} f(x + u\gamma) &= Tr\Big(H\big((x+u\gamma)^q - \gamma^{q-1}(x+u\gamma)\big) + \beta(x+u\gamma)\Big) \\ &= Tr\Big(H\big(x^q + u\gamma^q - \gamma^{q-1}x - u\gamma^q\big) + \beta x + u\beta\gamma)\Big) \\ &= Tr\Big(H\big(x^q - \gamma^{q-1}x\big) + \beta x\Big) + uTr(\beta\gamma) \\ &= f(x) + uTr(\beta\gamma). \end{aligned}$$

◇

Another family of mappings with known linear translators is given in the next lemma, which can be verified by direct calculations similarly to Lemma 1.

Lemma 2 *Let $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $\alpha \in \mathbb{F}_{q^n}^*$. Then for any $c \in \mathbb{F}_q^*$ the element $c\alpha$ is a 0-linear structure of*

$$f(x) = \sum_{u \in \mathbb{F}_q} g(x + u\alpha).$$

Lemma 3 *Let $n = 4k$, $\beta \in \mathbb{F}_{q^n}$ and $\gamma \in \lambda^{(q^{4k}-1)/2(q^2-1)}\mathbb{F}_{q^2}^*$ with λ being a primitive element of $\mathbb{F}_{q^n}$. Then γ is a $Tr\big(\beta\gamma\big)$-linear structure of*

$$f(x) = Tr(x^{q+1} + \beta\, x).$$

Proof. Note that $\gamma^{q^2-1} = -1$ or equivalently $\gamma^{q^2} + \gamma = 0$. Taking the latter identity to the power q^{n-1}, we obtain $\gamma^q + \gamma^{q^{n-1}} = 0$. Further, since $(\gamma^{q+1})^{q-1} = -1$, it holds $(\gamma^{q+1})^q + \gamma^{q+1} = 0$, and consequently $Tr(\gamma^{q+1}) = 0$. Using this properties of γ, for any $x \in \mathbb{F}_{q^n}$ and $u \in \mathbb{F}_q$ we obtain

$$\begin{aligned} f(x + u\gamma) &= Tr((x + u\gamma)^{q+1} + \beta x + \beta\gamma u) \\ &= Tr(x^{q+1} + \gamma^q u x + \gamma u x^q + \gamma^{q+1}u^2 + \beta x + u\beta\gamma) \\ &= f(x) + u\,Tr((\gamma^q + \gamma^{q^{n-1}})x) + u^2 Tr(\gamma^{q+1}) + uTr(\gamma\beta) \\ &= f(x) + uTr(\gamma\beta). \end{aligned}$$

◇

Lemmas 1, 2, as well as the Theorem 2, are straightforward generalizations of results given in [2] in the case of prime q. The proof of Theorem 2 differs from the one given in [2].

Theorem 2 *Let $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$.*

(a) Then $F(x) = x + \gamma\, f(x)$ is a permutation of $\mathbb{F}_{q^n}$ if $b \neq -1$.

(b) Then $F(x) = x + \gamma\, f(x)$ is a $q-$ to -1 mapping of $\mathbb{F}_{q^n}$ if $b = -1$.

Proof. Let $x, y \in \mathbb{F}_{q^n}$ satisfy $F(x) = F(y)$. Then

$$F(x) = x + \gamma\, f(x) = y + \gamma\, f(y) = F(y), \tag{4}$$

and hence

$$x = y + \gamma\ (f(y) - f(x)) = y + \gamma a,$$

where $a = f(y) - f(x) \in \mathbb{F}_q$. Using the definition of a linear translator we get

$$a = f(y) - f(x) = -\,(f(y + \gamma a) - f(y)) = -ab.$$

If $b \neq -1$, then the last equality implies $a = 0$ and hence $f(y) = f(x)$. Finally, (4) forces $x = y$, which proves (a). Suppose $b = -1$. Then the above arguments

show that $F(x) = F(y)$ only if $x = y + \gamma a$ for some $a \in \mathbb{F}_q$. To complete the proof of (b) it remains to see that

$$F(y + \gamma a) = y + \gamma a + \gamma f(y + \gamma a) = y + \gamma a + \gamma f(y) - \gamma a = F(y)$$

for any $a \in \mathbb{F}_q$. $\diamond$

If we choose $f(x) = Tr(x)$, then Theorem 2 states that the mapping $x \mapsto x + \gamma\, Tr(x)$ is a permutation of $\mathbb{F}_{q^n}$ if and only if $Tr(\gamma) \neq -1$. Consequently, the mapping $x \mapsto Tr(x) + \delta\, x$ is a permutation of $\mathbb{F}_{q^n}$ if and only if $\delta \neq 0$ and $Tr(\delta^{-1}) \neq -1$, and thus

$$\mathcal{M}(Tr) = \{\delta \in \mathbb{F}_{q^n}^* \mid Tr(\delta^{-1}) \neq -1\}.$$

In particular $|\mathcal{M}(Tr)| = q^n - q^{n-1} - 1$. The mapping $Tr(x)$ was mentioned in [10] to show that certain bounds on $|\mathcal{M}(\cdot)|$ are tight, see [1] for further details.

Let us consider an arbitrary $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. The mapping $f(x) + \delta x$ is a permutation of $\mathbb{F}_{q^n}$ if and only if $\delta \neq 0$ and $x + \delta^{-1} f(x)$ is a permutation. So by Theorem 2, the inverse of any b-linear translator δ^{-1} of f with $b = f(\delta^{-1}) - f(0) \neq -1$ is contained in $\mathcal{M}(f)$. So it holds

$$\{\delta \in \mathbb{F}_{q^n}^* \mid \delta^{-1} \in \Lambda^*(f) \ \text{ and } \ f(\delta^{-1}) - f(0) \neq -1\} \subseteq \mathcal{M}(f). \tag{5}$$

This shows that the mappings $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ with many linear translators determine few directions. The next result describes such mappings.

Theorem 3 *Let $g : \mathbb{F}_q \to \mathbb{F}_q$ be such that $g(0) = 0$ and $-1 \notin \{g(y) \mid y \in \mathbb{F}_q\}$. Given a non-zero $\alpha \in \mathbb{F}_{q^n}$ define $h : \mathbb{F}_{q^n} \to \mathbb{F}_q$ by $h(x) = g(Tr(\alpha x))$ for any $x \in \mathbb{F}_{q^n}$. Then $\{\delta \in \mathbb{F}_{q^n}^* \mid Tr(\alpha\delta^{-1}) = 0\} \subseteq \mathcal{M}(h)$ and hence $|\mathcal{M}(h)| \geq q^{n-1} - 1$.*

Proof. Theorem 1 implies that $\{y \in \mathbb{F}_{q^n}^* \mid Tr(\alpha y) = 0\} \subseteq \Lambda^*(h)$. Then from (5) it follows

$$\{\delta \in \mathbb{F}_{q^n}^* \mid g(Tr(\alpha\delta^{-1})) \neq -1 \text{ and } Tr(\alpha\delta^{-1}) = 0\} \subseteq \mathcal{M}(h).$$

It remains to note that

$$\{\delta \in \mathbb{F}_{q^n}^* \mid g(Tr(\alpha\delta^{-1})) \neq -1 \text{ and } Tr(\alpha\delta^{-1}) = 0\} = \{\delta \in \mathbb{F}_{q^n}^* \mid Tr(\alpha\delta^{-1}) = 0\}$$

since by the choice of g the element -1 does not belong to its image set. $\diamond$

Remark that if in Theorem 3 the mapping g is not affine on $\mathbb{F}_q$, then h is not affine on $\mathbb{F}_{q^n}$. Hence $\{y \in \mathbb{F}_{q^n}^* \mid Tr(\alpha y) = 0\} = \Lambda^*(h)$ for such mappings using Proposition 1. Next we give an explicit example of such a mapping h if q is odd.

Example 1 *Let q be odd and $q - 1 = 2^i \cdot d$ with d odd. Let $h : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be defined by*

$$h : x \mapsto \Big(Tr(x)\Big)^{2^i} \quad \textit{for any} \quad x \in \mathbb{F}_{q^n}.$$

Then $\{\delta \in \mathbb{F}_{q^n}^* \mid Tr(\delta^{-1}) = 0\} \subseteq \mathcal{M}(h)$.

It is obvious that the permutations described in Theorem 2 are never orthomorphisms, and hence never complete if q is even. Corollary 1 characterizes all such complete mappings.

Corollary 1 *Let q be odd and $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Then $F(x) = x + \gamma f(x)$ is a complete mapping of $\mathbb{F}_{q^n}$ if and only if $b \notin \{-1, -2\}$.*

Proof. Indeed F is a permutation if and only if $b \neq -1$ by Theorem 2. Consider $F(x)+x = 2x+\gamma f(x)$. The latter is a permutation of $\mathbb{F}_{q^n}$ if and only if $x+\frac{\gamma}{2} f(x)$ is so. Proposition 1 shows that $\gamma/2$ is a $b/2$-linear translator of f. Thus $F(x) + x$ is a permutation of $\mathbb{F}_{q^n}$ if and only if $b \neq -2$, completing the proof. ◇

Our next goal is to determine the cycle structure and the inverse of a permutation described in Theorem 2. For an integer $k \geq 1$, define

$$F_k(x) = \underbrace{F \circ F \circ \ldots \circ F}_{k \text{ times}}(x)$$

to be the k-fold composition of the mapping F with itself.

Lemma 4 *Let $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $F(x) = x + \gamma f(x)$. Then for any $k \geq 1$ it holds*

$$F_k(x) = x + B_k \gamma f(x),$$

where

$$B_k = 1 + (b+1) + \ldots + (b+1)^{k-1} = \begin{cases} k & \text{if } b = 0 \\ \frac{(b+1)^k - 1}{b} & \text{if } b \neq 0. \end{cases} \tag{6}$$

Proof. Our proof is by induction on k. Clearly it holds for $k = 1$. For $k \geq 2$ we have

$$\begin{aligned} F_k(x) &= F \circ F_{k-1}(x) = (x + \gamma f(x)) \circ (x + B_{k-1} \gamma f(x)) \\ &= x + B_{k-1} \gamma f(x) + \gamma f(x + B_{k-1} \gamma f(x)). \end{aligned}$$

Since γ is a b-linear translator for f and $B_{k-1} f(x) \in \mathbb{F}_q$, it holds

$$f(x + B_{k-1} \gamma f(x)) = f(x) + B_{k-1} f(x) b.$$

Then we get

$$F_k(x) = x + (B_{k-1} + 1 + B_{k-1} b)\gamma f(x) = x + (1 + (b+1)B_{k-1})\gamma f(x).$$

It remains to note that $1 + (b+1)B_{k-1} = B_k$. ◇

As a direct consequence of Lemma 4, we determine the inverse mapping and the cycle structure of the considered permutations.

Theorem 4 *Let $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $b \neq -1$. Then the inverse mapping of the permutation $F(x) = x + \gamma\, f(x)$ is*

$$F^{-1}(x) = x - \frac{\gamma}{b+1}\, f(x).$$

Proof. Let $b = 0$. Then from Lemma 4 it follows that $F_p(x) = x$ where p is the characteristic of $\mathbb{F}_{q^n}$. Hence the inverse mapping of F is $F_{p-1}(x) = x - \gamma\, f(x)$. Let $b \neq 0$. Then again using Lemma 4 the inverse mapping of F is F_{l-1}, where l is the order of $b+1$ in $\mathbb{F}_q^*$. It remains to note that

$$\begin{aligned} F_{l-1}(x) &= x + \frac{(b+1)^{l-1} - 1}{b}\, \gamma\, f(x) \\ &= x + \left(\frac{1}{b+1} - 1\right) \frac{1}{b}\, \gamma\, f(x) \\ &= x - \frac{\gamma}{b+1}\, f(x), \end{aligned}$$

since $(b+1)^{l-1} = (b+1)^{-1}$. ◇

Obviously, an element $u \in \mathbb{F}_{q^n}$ is a fixed point for $F(x) = x + \gamma f(x),\ \gamma \neq 0$, if and only if $f(u) = 0$. The next theorem describes the cycle decomposition of such permutations.

Theorem 5 *Let $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $b \neq -1$. Consider the permutation defined by $F(x) = x + \gamma\, f(x)$. Set*

$$N = q^n - |\{x \in \mathbb{F}_{q^n} \mid f(x) = 0\}|.$$

(a) If $b = 0$, then the permutation F is a composition of N/p disjoint cycles of length p (in the symmetric group $S_{\mathbb{F}_{q^n}}$), where p is the characteristic of $\mathbb{F}_{q^n}$. Moreover, an element $u \in \mathbb{F}_{q^n}$ with $f(u) \neq 0$ is contained in the cycle $(u_0, u_1, \ldots, u_{p-1})$, where $u_k = u + k\, \gamma f(u)$.

(b) If $b \neq 0$, then the permutation F is a composition of N/l disjoint cycles of length l, where l is the order of $(b+1)$ in $\mathbb{F}_q^*$. Moreover, an element $u \in \mathbb{F}_{q^n}$ with $f(u) \neq 0$ is contained in the cycle $(u_0, u_1, \ldots, u_{l-1})$, where $u_k = u + B_k\, \gamma f(u)$ and B_k is defined by (6).

Proof. The proof follows from Lemma 4. ◇

Remark 1 *A particular case of Corollary 1 and Theorem 4 for $b = 0$ are proved in [8] for permutations $x + h(Tr(x))$, where $h : \mathbb{F}_q \to \mathbb{F}_q$ and q is a prime number. In [8] and [11] further permutations of $\mathbb{F}_{q^n}$ involving additive mappings are constructed.*

3 Families of permutation polynomials

In this section we demonstrate several applications of Theorems 2 and 4 to obtain explicit constructions of permutation polynomials. Firstly, observe that combining Theorem 2 and Lemma 1 we obtain:

Theorem 6 *Let $H(X) \in \mathbb{F}_{q^n}[X],\ \gamma, \beta \in \mathbb{F}_{q^n}$. Then*

$$F(X) = X + \gamma\, Tr\big(H(X^q - \gamma^{q-1}X) + \beta X\big)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $Tr(\gamma\beta) \neq -1$.

Further families of permutation polynomials may be obtained using the following extension of Theorem 2.

Theorem 7 *Let $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linear permutation of $\mathbb{F}_{q^n}$. Further, suppose $\gamma \in \mathbb{F}_{q^n}$ is a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$.*

(a) Then $F(x) = L(x) + L(\gamma)\, f(x)$ is a permutation of $\mathbb{F}_{q^n}$ if $b \neq -1$.

(b) Then $F(x) = L(x) + L(\gamma)\, f(x)$ is a $q-$ to -1 mapping of $\mathbb{F}_{q^n}$ if $b = -1$.

Proof. Note that the mapping F is the composition of L and the mapping $x + \gamma\, f(x)$. Indeed,

$$L\big(x + \gamma\, f(x)\big) = L(x) + L\big(\gamma\, f(x)\big) = L(x) + f(x)L(\gamma).$$

The rest follows from Theorem 2.

$\diamond$

Recall that $\mathbb{F}_q$-linear mappings of $\mathbb{F}_{q^n}$ are described by the polynomials $\sum_{i=0}^{n-1} \alpha_i X^{q^i} \in \mathbb{F}_{q^n}[X]$, which are called q-polynomials. Hence given a permutation q-polynomial, Theorem 7 combined with Lemma 1 or Lemma 2 yields variety of families of permutation polynomials. As an example we consider $L(X) = X^q + X$, which is a permutation polynomial of $\mathbb{F}_{q^n}$ when n is odd. The inverse mapping of L is given by

$$L^{-1}(X) = X^{q^{n-1}} - X^{q^{n-2}} + \ldots + X^{q^2} - X^q + X.$$

Using these polynomials and Theorem 7, Lemma 1 we obtain:

Theorem 8 *Let $H(X) \in \mathbb{F}_{q^n}[X],\ \gamma, \beta \in \mathbb{F}_{q^n}$ and n be odd.*

(a) Then

$$X^q + X + (\gamma^q + \gamma)\, Tr\big(H(X^q - \gamma^{q-1}X) + \beta X\big)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $Tr(\gamma\beta) \neq -1$.

(b) Then

$$\sum_{i=1}^{n}(-1)^{i+1}X^{q^{n-i}} + \Big(\sum_{i=1}^{n}(-1)^{i+1}\gamma^{q^{n-i}}\Big)\,Tr\big(H(X^q - \gamma^{q-1}X) + \beta X\big)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $Tr(\gamma\beta) \neq -1$.

The following result is of interest if γ and δ are linearly independent over $\mathbb{F}_q$, otherwise it is covered by Theorem 2. It describes permutations of $\mathbb{F}_{q^n}$ obtained form the identity mapping by changing its $\gamma-$ and $\delta-$coordinate functions.

Theorem 9 *Let $\gamma, \delta \in \mathbb{F}_{q^n}$. Suppose γ is a b_1-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and a b_2-linear translator of $g : \mathbb{F}_{q^n} \to \mathbb{F}_q$, and moreover δ is a d_1-linear translator of f and a d_2-linear translator of g. Then*

$$F(x) = x + \gamma\, f(x) + \delta\, g(x)$$

is a permutation of $\mathbb{F}_{q^n}$, if $b_1 \neq -1$ and $d_2 - \frac{d_1 b_2}{b_1+1} \neq -1$.

Proof. Since $b_1 \neq -1$, the mapping $G(x) = x + \gamma\, f(x)$ is a permutation by Theorem 2. Then using Theorem 4, the inverse mapping of G is

$$G^{-1}(x) = x - \frac{\gamma}{b_1+1}\, f(x).$$

Consider

$$\begin{aligned} F \circ G^{-1}(x) &= G \circ G^{-1}(x) + \delta\, g(x - \frac{\gamma}{b_1+1}\, f(x)) \\ &= x + \delta\left(g(x) - \frac{b_2}{b_1+1} f(x)\right) \\ &= x + \delta\, h(x). \end{aligned}$$

Note that δ is a $\left(d_2 - \frac{d_1 b_2}{b_1+1}\right)$-linear translator of $h : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Indeed, for any $u \in \mathbb{F}_q$ it holds

$$\begin{aligned} h(x+\delta u) &= g(x+\delta u) - \frac{b_2}{b_1+1} f(x+\delta u) \\ &= g(x) + d_2 u - \frac{b_2}{b_1+1}(f(x) + d_1 u) \\ &= h(x) + \left(d_2 - \frac{d_1 b_2}{b_1+1}\right) u. \end{aligned}$$

Theorem 2 completes the proof. ◇

As an application of Theorem 9 we obtain:

Theorem 10 *Let $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ and*

$$M(X) = X^{q^2} - (1 + (\alpha^q - \alpha)^{q-1})X^q + (\alpha^q - \alpha)^{q-1}X.$$

Let $H_1, H_2 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and $\beta_1, \beta_2 \in \mathbb{F}_{q^n}$ be arbitrary. Then

$$F(X) = X + Tr\big(H_1(M(X)) + \beta_1 X\big) + \alpha\, Tr\big(H_2(M(X)) + \beta_2 X\big)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if

- *$Tr(\beta_1) \neq -1$ and $Tr(\alpha\beta_2) - \frac{Tr(\alpha\beta_1)Tr(\beta_2)}{Tr(\beta_1)+1} \neq -1$; or*
- *$Tr(\alpha\beta_2) \neq -1$ and $Tr(\beta_1) - \frac{Tr(\beta_2)Tr(\alpha\beta_1)}{Tr(\alpha\beta_2)+1} \neq -1$.*

Proof. We are in the setting of Theorem 9: In the first case, $\gamma = 1,\ \delta = \alpha$ and $f(x) = Tr\big(H_1(M(x)) + \beta_1 x\big),\ g(x) = Tr\big(H_2(M(X)) + \beta_2 X\big)$. Direct calculations show that 1 is a $Tr(\beta_1)$-linear translator of f and is a $Tr(\beta_2)$-linear translator of g, since $M(1) = 0$. Similarly, δ is a $Tr(\delta\beta_1)$-linear translator of f and is a $Tr(\delta\beta_2)$-linear translator of g. In the second case the roles of f and g are exchanged. ◇

4 Further constructions

The results of this section are inspired by Theorem 1 from [8] and meanwhile generalize it and most of the constructions of permutations from [2].

Theorem 11 *Let $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $h : \mathbb{F}_q \to \mathbb{F}_q$. Define $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ by*

$$F(x) = x + \gamma\, h(f(x)).$$

Then F permutes $\mathbb{F}_{q^n}$ if and only if the mapping $g(u) = bh(u) + u$ permutes $\mathbb{F}_q$.

Proof. The arguments from the proof of Theorem 2 show that if for some $x, y \in \mathbb{F}_{q^n}$ it holds $F(x) = F(y)$, then $x = y + \gamma a$ with $a \in \mathbb{F}_q$. Further, $F(y) = F(y + \gamma a)$ implies

$$y + \gamma a + \gamma\, h(f(y) + ba) = y + \gamma\, h(f(y)), \tag{7}$$

since

$$F(y + \gamma a) = y + \gamma a + \gamma\, h(f(y + \gamma a)) = y + \gamma a + \gamma\, h(f(y) + ba).$$

Equation (7) is equivalent to

$$a + h(f(y) + ba) = h(f(y)). \tag{8}$$

If $b = 0$ then from (8) forces $a = 0$ and hence the statement is true for that case. If $b \neq 0$, then (8) can be reduced to

$$h(f(y) + ba) + b^{-1}\big(f(y) + ba) = h(f(y)) + b^{-1}f(y),$$

and hence $g(f(y) + ba) = g(f(y))$. The latter equation is satisfied only for $a = 0$ if and only if g is a permutation of $\mathbb{F}_q$.

$\diamond$

Observe that Theorem 2 follows from Theorem 11 if we take g to be the identity mapping. Next family of permutation polynomials is obtained combining Theorem 11 and Lemma 3.

Theorem 12 *Let $n = 4k$, $\beta \in \mathbb{F}_{q^n}$ and $\gamma \in \lambda^{(q^{4k}-1)/2(q^2-1)}\mathbb{F}_{q^2}^*$ with λ being a primitive element of $\mathbb{F}_{q^n}$. Further, suppose t is a positive integer with $\gcd(t, q-1) = 1$. Then the polynomial*

$$F(X) = X + \gamma\, Tr(\gamma\beta)^{q-2}\left(\big(Tr(X^{q+1} + \beta x)\big)^t - Tr(X^{q+1} + \beta x)\right)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$.

Proof. We apply Theorem 11 with $h(u) = Tr(\gamma\beta)^{q-2}(u^t - u)$ and $f(x) = Tr(x^{q+1} + \beta x)$. Lemma 3 shows that γ is a $Tr(\gamma\beta)$-linear translator of f. To complete the proof note that the mapping

$$Tr(\gamma\beta)h(u) + u = \begin{cases} u & \text{if } Tr(\gamma\beta) = 0 \\ u^t & \text{otherwise,} \end{cases}$$

and thus h is a permutation of $\mathbb{F}_q$. $\diamond$

Theorem 13 *Let $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linear permutation of $\mathbb{F}_{q^n}$. Let $\gamma \in \mathbb{F}_{q^n}$ be a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $h : \mathbb{F}_q \to \mathbb{F}_q$. Then the mapping*

$$G(x) = L(x) + L(\gamma)\, h(f(x))$$

permutes $\mathbb{F}_{q^n}$ if and only if $g(u) = bh(u) + u$ permutes $\mathbb{F}_q$.

Proof. Note that G is a composition of L and $F(x) = x + \gamma\, h(f(x))$. Indeed,

$$L\big(x + \gamma\, h(f(x))\big) = L(x) + h(f(x))L(\gamma).$$

The rest of the proof follows from Theorem 11.

$\diamond$

Next we show that Theorem 1 of [8] is a particular case of Theorem 13.

Theorem 14 ([8]) *Let $L(X) \in \mathbb{F}_q[X]$ be a permutation polynomial of $\mathbb{F}_{q^n}$, $h(X) \in \mathbb{F}_q[X]$ and $\gamma \in \mathbb{F}_{q^n}$ with $Tr(\gamma) = b$. Then the polynomial*

$$L(X) + \gamma\, h\big(Tr(X)\big)$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if the polynomial

$$L(1)X + bh(X)$$

is a permutation polynomial of $\mathbb{F}_q$.

Proof. Since L is a permutation of $\mathbb{F}_{q^n}$ there is a unique $\delta \in \mathbb{F}_{q^n}$ such that $L(\delta) = \gamma$. Note that δ is a $Tr(\delta)$-linear translator of the mapping $Tr(x)$. Moreover, if $L(X) = \sum_{i=0}^{n-1} a_i X^{q^i}$, then

$$Tr(\gamma) = Tr(L(\delta)) = Tr(\sum_{i=0}^{n-1} a_i \delta^{q^i}) = \sum_{i=0}^{n-1} a_i Tr(\delta) = L(1)Tr(\delta),$$

and hence $Tr(\delta) = (L(1))^{-1}b$. The rest follows from Theorem 13. ◇

Finally, we describe permutation polynomials obtained from $\mathbb{F}_q$-linear mappings of $\mathbb{F}_{q^n}$ with one-dimensional kernel via changing a coordinate function.

Theorem 15 *Let $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linear mapping of $\mathbb{F}_{q^n}$ with kernel $\alpha\mathbb{F}_q$, $\alpha \neq 0$. Suppose α is a b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and $h : \mathbb{F}_q \to \mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Then the mapping*

$$G(x) = L(x) + \gamma\, h(f(x))$$

permutes $\mathbb{F}_{q^n}$ if and only if $b \neq 0$ and γ does not belong to the image set of L.

Proof. In the case γ belongs to the image set of L, the image set of G is contained in that of L. Hence if G is a permutation, then necessarily γ is not in the image of L. Now suppose, γ does not belong to the image set of L. Let $x, y \in \mathbb{F}_{q^n}$ be such that $G(x) = G(y)$. Then

$$L(x) + \gamma\, h(f(x)) = L(y) + \gamma\, h(f(y)),$$

and consequently

$$\gamma\Big(h(f(x)) - h(f(y))\Big) = L(y - x). \tag{9}$$

Since γ does not belong to the image set of L, equation (9) is possible if and only if $h(f(x)) = h(f(y))$ and $y - x$ is in the kernel of L. So, let $y = x + a\alpha$ with $a \in \mathbb{F}_q$. Then (9) is reduced to

$$h(f(x)) - h(f(x + a\alpha)) = h(f(x)) - h(f(x) + ab) = 0. \tag{10}$$

The only solution of (10) is $a = 0$ if and only if $b \neq 0$ and h permutes $\mathbb{F}_q$.

$\diamond$

A particular case of Theorem 15, where the mapping h is the identity mapping, is proved in [2]. As an application of Theorem 15 we describe a family of permutation polynomials.

Theorem 16 *Let t be a positive integer with $\gcd(t, q-1) = 1$, $H(X) \in \mathbb{F}_{q^n}[X]$ and $\gamma, \beta \in \mathbb{F}_{q^n}$. Then*

$$G(X) = X^q - X + \gamma\Big(Tr(H(X^q - X) + \beta X)\Big)^t \in \mathbb{F}_{q^n}[X]$$

is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if $Tr(\gamma) \neq 0$ and $Tr(\beta) \neq 0$.

Proof. We apply Theorem 15 with $L(x) = x^q - x$, $f(x) = Tr(H(x^q - x) + \beta x)$ and $h(u) = u^t$. The mapping $L(x) = x^q - x$ is $\mathbb{F}_q$-linear with kernel $\mathbb{F}_q$ and so α may be chosen to be 1. The image set of L consist of all elements y from $\mathbb{F}_{q^n}$ with $Tr(y) = 0$ by Hilbert's Theorem 90. Further $\alpha = 1$ is a $Tr(\beta)$-linear translator of the mapping $f(x)$. Indeed, for any $u \in \mathbb{F}_q$ it holds

$$\begin{aligned} f(x+u) &= Tr(H((x+u)^q - (x+u)) + \beta(x+u)) \\ &= Tr(H(x^q - x) + \beta x) + u\,Tr(\beta) \\ &= f(x) + u\,Tr(\beta). \end{aligned}$$

It remains to note that $h(u) = u^t$ is a permutation of $\mathbb{F}_q$ by the choice of t. $\diamond$

Acknowledgments

The author thanks Pascale Charpin and Mike Zieve for their comments on the preliminary version of this paper.

References

[1] S. Ball, The number of directions determined by a function over a finite field, *J. Combin. Theory Ser. A*, 104, pp. 341–350 (2003).

[2] P. Charpin and G. Kyureghyan, When does $F(X) + \gamma Tr(H(X))$ permute $\mathbf{F}_{p^n}$? submitted, 2008.

[3] P. Charpin and G. Kyureghyan, On a class of permutation polynomials over $\mathbf{F}_{2^n}$, In *SETA 2008*, LNCS 5203, pp. 368-376, Springer-Verlag (2008).

[4] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, *Adv. in Math. of Communications* 3(1), pp. 59-81 (2009).

[5] R. J. Evans, J. Greene, and H. Niederreiter, Linearized polynomials and permutation polynomials of finite fields, *Michigan Math. J.*, 39(3), pp. 405–413 (1992).

[6] X. Lai, Additive and linear structures of cryptographic functions, *Proc. of FSE*, LNCS 1008, pp. 75-85 (1995).

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications 20.

[8] J. E. Marcos, Specific permutation polynomials over finite fields, *Finite Fileds and their Applications*, in press (2009).

[9] H. Niederreiter and K.H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc.* (Series A) 33, pp. 197-212 (1982).

[10] L. Rédei, *Lückenhafte Polynome über endlichen Körpern*, Birkhäuser Verlag, Basel (1970).

[11] M. E. Zieve, *Classes of Permutation Polynomials Based on Cyclotomy and an Additive Analogue*, arXiv:0810.2830v1.